Dalle *Disquisitiones Arithmeticae* di Carl Friedrich Gauss (1801)

SECTIO PRIMA

DE

NUMERORUM CONGRUENTIA IN GENERE.

Numeri congrui, moduli, residua et nonresidua.

1.

Si numerus a numerorum b, c differentiam metitur, b et c *secundum a congrui* dicuntur, sin minus, *incongrui*: ipsum a *modulum* appellamus. Uterque numerorum b, c priori in casu alterius *residuum*, in posteriori vero *nonresiduum* vocatur.

Hae notiones de omnibus numeris integris tam positivis quam negativis *) valent, neque vero ad fractos sunt extendendae. *E. g.* -9 et $+16$ secundum modulum 5 sunt congrui; -7 ipsius $+15$ secundum modulum 11 residuum, secundum modulum 3 vero nonresiduum. Ceterum quoniam cifram numerus quisque metitur, omnis numerus tamquam sibi ipsi congruus secundum modulum quemcunque est spectandus.

2.

Omnia numeri dati a residua secundum modulum m sub formula $a + km$ comprehenduntur, designante k numerum integrum indeterminatum. Propositionum quas post trademus faciliores nullo negotio hinc demonstrari possunt: sed istarum quidem veritatem aeque facile quivis intuendo poterit perspicere.

*) Modulus manifesto semper *absolute* i. e. sine omni signo est sumendus.

2

Numerorum congruentiam hoc signo, $\equiv$, in posterum denotabimus, modulum ubi opus erit in clausulis adiungentes, $-16 \equiv 9$ (mod. 5), $-7 \equiv 15$ (mod. 11) *).

<u>Versione italiana:</u>

SEZIONE PRIMA

DELLA CONGRUENZA DEI NUMERI IN GENERE

1.

*Se il numero a misura la differenza dei numeri b, c, b e c vengono detti **congrui** secondo a, altrimenti incongrui. Chiamiamo **modulo** questo a. Ognuno dei due numeri viene detto nel primo caso **residuo**, nel secondo caso **non residuo** dell'altro.*
Queste nozioni valgono per tutti i numeri interi, sia positivi sia negativi *), *ma non possono essere estese ai numeri frazionari. Così, ad esempio,* -9 *e* +16 *sono congrui modulo* 5, -7 *è modulo* 11 *residuo, ma modulo* 3 *non residuo di* +15. *Poiché inoltre lo zero è misurato da qualsiasi numero, ogni numero è da considerarsi congruo a se stesso secondo qualunque modulo.*

*)*Evidentemente il modulo si prende sempre in modo assoluto, ossia senza segno.*

2.

Tutti i resti di un numero assegnato a secondo il modulo m sono contenuti nella formula a+km, in cui k denota un numero intero indeterminato. Delle proposizioni che successivamente stabiliremo, le più facili si possono derivare senza sforzo da qui; tuttavia chiunque potrà riconoscere la loro correttezza altrettanto facilmente a prima vista.
Nel seguito denoteremo la congruenza dei numeri con il segno ≡ e, laddove necessario, aggiungendo il modulo tra parentesi: $-16 \equiv 9 \pmod{5}$, $-7 \equiv 15 \pmod{11}$.

<u>Nota linguistica:</u> La parola latina ***modulus*** è il diminutivo di *modus*, che significa *misura*. Da qui è passato, nel moderno gergo della matematica, a introdurre qualsiasi criterio che porti a identificare due oggetti di per sé distinti, in qualche senso "ignorando" una loro parte: nel caso dei numeri interi congrui *modulo* il numero intero positivo n, ad essere ignorati sono i massimi multipli di n che essi "contengono": più precisamente, se $a = nq + r$ è l'espressione della divisione euclidea dell'intero a per n, si ignora nq. In effetti, per ogni altro intero b, si ha che $a \equiv b \pmod{n}$ se e solo se a e b hanno lo stesso resto r nella divisione euclidea per n. Infatti, se $b = nq' + r'$ è l'espressione della divisione euclidea di b per n, allora n divide la differenza $a - b = n(q - q') + r - r'$ se e solo se n divide $r - r'$. Dato che il valore assoluto di questo numero è minore di n, ciò vale se e solo se $r = r'$. Questa osservazione giustifica il termine ***residuum*** (sinonimo di *resto*) adottato da Gauss.

Di seguito, un facile quesito basato su altri due risultati contenuti nella stessa opera.

A quali proprietà enunciate nelle Lezioni 8 e 9 del corso di Algebra si riferiscono le seguenti affermazioni?

23.

Si a ad m primus, et e, f numeri secundum modulum m incongrui: erunt etiam ae, af incongrui secundum m.

23.

Se a è coprimo con m, ed e,f sono numeri incongrui secondo il modulo m, allora anche ae, af saranno incongrui secondo il modulo m.

24.

***Expressio** $ax+b$*, denotantibus a, b numeros datos, x numerum indeterminatum seu variabilem, *secundum modulum m, ad a primum, cuivis numero dato congrua fieri potest.*

24.

L'espressione $ax+b$, in cui a, b denotano numeri assegnati, e x un numero indeterminato o variabile, può essere reso congruo, secondo il modulo m, coprimo con a, a qualsiasi numero assegnato.